

DIR Contract Number: DIR-MSS-SCP-001

**Appendix 8 to
Tenth Amendment of
Master Services Agreement**

**Attachment 13-A
Description of Reports**

January 15, 2021



**Attachment to Managed Security Services
Service Component Provider
Master Services Agreement
DIR Contract No. DIR-MSS-SCP-001**

Between

**The State of Texas, acting by and through
the Texas Department of Information Resources**

and

AT&T Corp.

**Attachment 13-A
Description of Reports**

January 15, 2021

Change Log			
CCR	Amendment	Date	Description of Change
CCR-000278	N/A	13-Jun-18	Deleted rows 36 through 56, revised row 59, revised rows 74 through 76, added 15 reports to the "Security Monitoring and Device Management" section (beginning on row36), added & corrected data for Report IDs (column C), Report Location (column I), New or Existing Report (column K), and the RACI columns O and P of the "STC Reports" worksheet.
CCR-000329	Amendment 2	12-Dec-18	Updates made to align with new MSI contract. Changes include additions, deletions, and changes to reports. Added: -Monthly Incident Management Report -Enterprise Event Management Report -Pool and Rate Card Report -RCA Report -Problem Management Report -Asset Inventory Summary Report -Capacity Management Report -Digital Availability Plan -All Open Changes - at Customer and Enterprise Levels -Key Performance Indicators -Operating Measurements -Monthly Security Status Review -Monthly On-boarding/Off-boarding Report -Access Management Report -Security Initiative Reports -DIR Board Report -Monthly Operations Statistics Dashboard - DCS, MAS, MSS, Texas.gov -Open Project Status Report Removed: -DR Test Results report removed -RU Forecast Report removed -Individual Monthly Reports for Key Measures -Various reports and data required to validate SLAs -Revised: Description of Monthly Service Provider Scorecard Description of STC-OPS-SLA01
CCR-000350	Amendment 4	26-Jun-19	Adds: - Account Access Report for DIR's Statewide Portal for Enterprise Cybersecurity Threat, Risk and Incident Management (SPECTRIM) System for local government entities; - Application Availability Report for DIR's Statewide Portal for Enterprise Cybersecurity Threat, Risk and Incident Management (SPECTRIM) System for local government entities.
CCR-000419	Amendment 7	26-Jun-19	Removes: - Account Access Report for DIR's Statewide Portal for Enterprise Cybersecurity Threat, Risk and Incident Management (SPECTRIM) System for local government entities; - Application Availability Report for DIR's Statewide Portal for Enterprise Cybersecurity Threat, Risk and Incident Management (SPECTRIM) System for local government entities.
CCR-000437	Amendment 8	23-Oct-20	Adds: • Tab "STC Reports": - Operational Reports for Endpoint Detection and Response (EDR) Services; - Configuration Reports for Endpoint Detection and Response (EDR) Services.
CCR-000XXX	Amendment 10	15-Jan-21	• Tab "Change Log" - Corrects formatting of CCR numbers (Column B, Rows 5-9) • Tab "STC Reports" - Adds Advanced Threat Hunting One-Time Scan Report and Advanced Threat Hunting Subscription Report to Security Monitoring and Device Management report category (Rows 81 & 82).

Overview

This Attachment contains a summary description of the format, content, and frequency of key reports required by DIR and Customer. **NOTE: The reports listed under the following Report Categories apply to all Service Components: Scorecard; Finance; CMDDB/Software Reports; SLAs; and, Strategic.**

Column Name	Column Description
Contract Reference	MSA reference, if applicable
Report Category	Functional Category
Report ID	Identification title of the report
Report Name	Name of report
Description	Short description of the report and report content
Milestone Deliverable Date (if other than Commencement)	The milestone deliverable date for each report
Frequency	How often the report is distributed.
Recipient	DIR or Customer for whom report is created.
Report Location	Where the report is published ; Portal, email etc...
Report Generator Tool	Tool from which the Service Provider creates the report
New or Existing Report	If the report is currently provided by the Existing or being requested New
Report Data and Creation	Each column indicates which Service Component Provider provides the data for the report and which Service Component Provider creates the report.
Report Start Date (if other than Commencement)	The starting date for each report after Commencement Date.

											Report Data and Creation MSI publishes all reports. Column indicates who: (C) creates report for publication, (D) provides data to MSI			
Contract Reference	Report Category	Report ID	Report Name	Description	Frequency	Recipient	Report Location	Report Generator Tool	Existing or New Report	Report Start Date	MSI	Security Monitoring and Device Management	Incident Response	Risk and Compliance
	Scorecard													
		STC-OPS-SCD01	Monthly Service Provider Scorecard	Service Delivery Solution Group approved Customer's Scorecard of the Service Provider's performance.	Monthly	DIR, Customer	Web Portal	ServiceNow	Modification of Existing	Commencement Date	C,D	D	D	D
	Finance													
		STC-OPS-FIN01	DIR Shared Services DIR Invoice	DIR Invoice.	Monthly	DIR, Finance	Email, Web Portal	ITFM	Existing	Commencement Date	C,D	D	D	D
		STC-OPS-FIN03	HUB Spend Report	Tracks spending by Service Provider with HUB-qualified subcontractors.	Monthly	DIR, Finance and DIR HUB Coordinator	Web Portal in a downloadable format	Excel	Existing	Commencement Date	C,D	D	D	D
		STC-OPS-FIN05	Invoice Detail Reports	Various detail supporting the Service Provider Invoice for Services (various CMDB extracts; PPA detail; and HSC details).	Monthly	DIR, Finance	Web Portal in a downloadable format	ITFM	Existing	Commencement Date	C,D	D	D	D
	Asset Reports													
MSI 2.1 A.3.8.1		STC-OPS-SOFTW01	Software Installs and Upgrades Applied	Understand what changes have been made to H/W from a Software perspective. Provide a list of installs and upgrades that have been performed and the H/W those installs and upgrades were made upon.	Monthly	DIR, Customer	Web Portal	ServiceNow	Existing	Commencement Date	C,D	D	D	D
			Asset Inventory Summary Report	Provide integrated Asset Inventory reports in a formats agreed with DIR at various aggregated levels by Customer, STC MSI and Third Party Vendor that, at a minimum, includes: Provides statistics, lists and charts illustrating the assets in the STC supported environment. Provides a summary with drill-down details of all assets. Provides DQM reconciliation summary and detail reports with the inputs, processing and outputs from the DQM reconciliation process Provides reports on Incidents, Problems and Changes by asset.	Weekly	DIR	Web Portal	ServiceNow	New		C,D	D	D	D
	Capacity Management Responses													
			Capacity Management Report	Publish regular Capacity Management reports to Customers, which at a minimum will include current/recent utilization (and trends) compared to normal utilization, Service Levels, and previously identified baselines. Produce monthly reports on the current usage of resources, trends and forecasts and exceptions, in a format agreed to by DIR, that at a minimum includes the following: enabling visibility into the overall service health performance and trends based on utilization, availability, and technology currency Visibility into capacity-related Incidents and Problems	Monthly	DIR, Customer	Web Portal	ServiceNow	New		C, D	D	D	D
			Digital Availability Plan	Provide a monthly report in a format agreed upon with DIR that, at a minimum, includes the following: Compare performance and Availability statistics for each Application/environment with planned performance and Availability. Provide a list of all Outages by DIR Customer, linked to an Incident, including the date and time the Outage commenced, its duration, and the affected infrastructure and Applications. Provide trend analysis of the performance for each Application and Environment during the thirteen (13) most recent months Report on proposed preventative maintenance activities. Provide DIR with recommendations of preventative maintenance options. Provide regular reporting with respect to the following measures for all services and components for both current reporting period and trend over the prior twenty-four (24) months, and make available through the Portal: Number and impact of instances of unavailability. Mean time to restore. Mean time between Service/System Incidents. Mean time between failure. Provide regular reporting on the Availability of Service Management Systems (e.g. Incident Management, Request Management, Capacity Management) and the impact on Service Provider(s) ability to provide Services.	Monthly	DIR, Customer	Web Portal	ServiceNow	New		C, D	D	D	D

											Report Data and Creation MSI publishes all reports. Column indicates who: (C) creates report for publication, (D) provides data to MSI			
Contract Reference	Report Category	Report ID	Report Name	Description	Frequency	Recipient	Report Location	Report Generator Tool	Existing or New Report	Report Start Date	MSI	Security Monitoring and Device Management	Incident Response	Risk and Compliance
	Change Management													
			All Open Changes at Customer and Enterprise Levels	Report all Open changes, high risk, past Due, three month look ahead. Includes at a minimum a breakdown of metrics by type, category, priority, effected service or system, and success/failure. Provide integrated CAB reports containing all changes (both digitally and traditionally managed) in a format agreed with DIR that, at a minimum, includes: The status of all Changes active at the beginning of the week and all Changes raised during the week. The Changes to be implemented the following week. The Changes submitted for approval. Change Advisory Board method used for review and approval (e.g., digital CAB, traditional meeting) Provide statistical reporting on change activity to DIR as requested. Maintain a list of changes reclassified as standard and associated justification. This report will offer filtered visibility to allow a Customer-specific view or an Enterprise view based on organizational role.	Daily/ Monthly	DIR, Customer	Web Portal	ServiceNow	Modification of Existing		C,D	D	D	D
	Incident Reports													
			Monthly Incident Management Report	Key issues relating to Incident Management processes. Number of Incidents during the month, grouped by severity, service, agency, region, classification or other criteria as appropriate. List of Incidents, short description, reference number, and a shortcut to detailed description. Detailed description, including timing of activities. Links to Problems and Known Errors. Trend analysis of the Incidents reported during the thirteen (13) most recent months. Calculate metrics and provide monthly reports to DIR and Customers, which include: The number of Incidents. Sources of the Incidents. Frequency regarding the types or categories of Incidents. The duration of open Incident (average and quantities by age). Number and percentage of Incidents Resolved upon first contact. Trending metrics in terms of MTTRS (mean time to restore service) by category, priority and by service or SLA. Number and percentage of SLA impacting Incidents. Number and percentage of Incidents (by category, priority, service and SLA) that were handled within the SLA targets. Number and percentage of Incidents (by category, priority, service and SLA) reopened. Number and percentage of Incidents (by category, priority, service and SLA) reoccurring. Number and percentage of Incidents that have resulted in the creation of problem records. Percentage (by category, type and priority) of Incidents that were resolved by use of an Incident Model. Number and percentage of Incidents escalated by organization, category, priority and Service. The association of Incidents by cause and resolution by Service Component. Other pertinent information regarding Incident Resolution, including Service Level measurement reporting.	Monthly	DIR, Customer	Web portal	ServiceNow	New		C,D	D	D	D
			Enterprise Event Management Report	Provides statistics, lists and charts illustrating the Events collected in the STC supported environment including the number of, source, destination and type of event. Provides reports on Incidents and Problems initiated by the Enterprise Event Management system with trends over the past 13 months. Number of events per CIs. Number of occasions when an event is collected and can't be matched with a C1 Summary and details of events which resulted in an automated correction made to remediate errors. Statistical information about the number of, source, destination and type of event	Weekly	DIR	Web portal	ServiceNow	New		C,D	D	D	D
	Project Reports													
		DCS-OPS-PROJ02	Pool and Rate Card Report	Rate Card consumption of actual hours and associated costs for any projects/requests that are billed via a Rate Card (by project/request and by Customer) for all Shared Services, including MSI and SCP rate card resources.	Monthly	DIR	Web Portal Email	ServiceNow	New		C,D	D	D	D
			Open Project Status Report	Status report will include, at a minimum, the following: (a) any milestones achieved; (b) any variances to the schedule set forth in the applicable Service Proposal; (c) if the Project is behind schedule, a recovery plan that describes the actions that Service Provider will undertake in order to return to such schedule; (d) Deliverables and other Work Product that have been created, developed, and/or completed, in whole or in part, pursuant to the Service Proposal or otherwise as part of the Project and the status of each such Deliverable and other Work Product; (e) variances, if any, to the specifications of the Project; (f) any charges incurred to date, including hardware, software, labor and any other charges associated with the performance of the Project and execution of the Service Proposal, to the extent that such charges are relevant to STC Customer's payment obligations; (g) an identification of any potential known or reasonably anticipated risks regarding the Project (such as potential disruptions to STC Customer operations), and the actions that would need to be taken in order to mitigate and/or eliminate such risks; and (h) any relevant issues identified by either Party since the previous report.	Weekly	DIR, STC Customer	Web Portal	ServiceNow	New		C,D	D	D	D

											Report Data and Creation MSI publishes all reports. Column indicates who: (C) creates report for publication, (D) provides data to MSI			
Contract Reference	Report Category	Report ID	Report Name	Description	Frequency	Recipient	Report Location	Report Generator Tool	Existing or New Report	Report Start Date	MSI	Security Monitoring and Device Management	Incident Response	Risk and Compliance
	RCA Reports													
		DCS-OPS-RCA01	RCA Report	Summary RCA Tracking Report.	Weekly	DIR, Customer	Web Portal	ServiceNow	New		C,D	D	D	D
		DCS-OPS-RCA02	Problem Management Report	Percentage and number of Problems in total and grouped by category, priority, severity, status, DCS Customer, system/component, region, classification or other criteria as appropriate. Report to include: Statistics on total numbers of Problems. Logged (by requestor, site, category, summary, detail) Outstanding (by assigned group, assigned manager, assigned owner, category, site, status, summary, detail, aging timeframe) Completed (by assigned group, assigned manager, assigned owner, category, site, status, summary, detail, resolution timeframe, within target timeframe, outside of target timeframe). Repeat Problems. SLA Performance. Problem trends and analysis. The percentage and number of Problems and Corrective Actions in total and grouped by category, priority, severity, status, Customer, system/component, region, classification or other criteria as appropriate. Information regarding Major Problem Reviews, including all details set out above. Information regarding Problem analyses and RCAs conducted in the previous period. Problem trend analysis findings. Information regarding new Known Error records and/or workarounds added to the Known Error Database / Knowledge Database (including number, category, priority, etc.). Details on the use and utility of the Known Error Database / Knowledge Database. Details regarding open Problem / Known Error, including identification number, description, status, date/time of record open, status description, etc. Results of reviews of Incidents to identify recurring Incidents and associated Problems. Tracking information as to escalations, contacts, follow-ups and commitments. Tracking information as to requests from DIR and Customers' to initiate Problem Management. Any issues relating to the Problem Management process, such as any information that may improve or facilitate a better Problem Management process, including decisions to be made by DIR and Service Provider. Trend analysis of Problems reported during the thirteen (13) most recent months.	Monthly	DIR, Customer	Web Portal	ServiceNow	New	C,D	D	D	D	
	Performance Models													
		STC-OPS-SLA01	Monthly Service Level Compliance Report	The published compliance report will capture all service level data, including all Key Measures and Critical Service Levels, and it will be viewable at both the Enterprise and Customer level.	Monthly	DIR	Web Portal	ServiceNow	New		C,D	D	D	D
			Key Performance Indicators	Aggregation of Operating Measurements which represent the health of the Shared Services Program.	Monthly	DIR	Web Portal	ServiceNow	New		C,D	D	D	D
			Operating Measurements	Set of metrics that support business and strategic objectives	Monthly	DIR	Web Portal	ServiceNow	New		C,D	D	D	D
	Security													
		DCS-OPS-SEC03	Monthly Security Status Review	Roll-up of multiple sources: Monthly Security Updates Monthly Mainframe Security Services Monthly Identity and Access Management Services status report Monthly Background Checks TDCJ and DFPS status report Monthly Documentation and Process status reports (PPM updates, ISeC updates, etc.) Monthly ISeC status reports (number of exceptions, number pending, DCS Customer issues with ISeC implementation (delays in implementation, DCS Customer failure to submit exceptions, etc.) Monthly Antivirus/Malware status report Monthly Security Reports information derived from ISS Security Services	Monthly	DIR	Web Portal	PowerPoint	New		C,D	D	D	D
		DCS-OPS-SEC09	Monthly On-boarding/Off-boarding Report	Identify new personnel on-boarded and off-boarded personnel.	Monthly	DIR	Web Portal	ServiceNow	New		C,D	D	D	D
			Access Management Report	Report on all Access Requests and their status, access rights granted or removed, approver and dates of the request lifecycle.	Quarterly	DIR, Customer	Web Portal	ServiceNow	New		C,D	D	D	D
			Security Initiative Reports	Current status reports of any security initiatives. Criteria dependent on the initiative	Weekly	DIR	Web Portal	ServiceNow	New		C,D	D	D	D

											Report Data and Creation MSI publishes all reports. Column indicates who: (C) creates report for publication, (D) provides data to MSI			
Contract Reference	Report Category	Report ID	Report Name	Description	Frequency	Recipient	Report Location	Report Generator Tool	Existing or New Report	Report Start Date	MSI	Security Monitoring and Device Management	Incident Response	Risk and Compliance
	Executive & Leadership													
			DIR Board Report	Executive level Report on metrics and statistics for all Shared Services Programs - DCS, MSS, MAS, Texas.gov	Quarterly, As Needed	DIR	Email	ServiceNow	New		C,D	D	D	D
			Monthly Operations Statistics Dashboard - DCS, MAS, MSS, Texas.gov	Dashboard report showing operational statistics for Shared Services Programs. Report to include, but not limited to, SLA results, Scorecard results, HW currency, SW currency and forecast, Operational statistics.	Monthly	DIR	Email	ServiceNow	New		C,D	D	D	D
	Security Monitoring and Device Management													
		STC-OPS-SMDM01	SMDM - Statistical Reports	Executive level report showing trends based on defined SMDM operational and configuration reports	Monthly	DIR	MSI Portal	Word	New	10/1/2018	C	D		
		STC-OPS-SMDM02	Endpoint Device Services - Operational Reports	Metrics of all scans conducted to include, at a minimum: number of unique devices scanned; scan dates; name of instance or device; total number of events; number of file deletions; and, number and disposition of quarantined records across all devices.	Daily	DIR, Customer	MSI Portal	Word	New	At the frequency defined after the implementation of the first customer		C		
		STC-OPS-SMDM03	Endpoint Device Services - Configuration Reports	Metrics on Malware infections and remediation Number of exclusions (i.e., files, file types, folders, partitions, etc. that are excluded from the scan), number of new exclusions, number of exclusions removed and business justification for all exclusions. Report showing definition files and currency levels of the devices, e.g., definition files at N/N+1 levels	Weekly	DIR, Customer	MSI Portal	Excel	New	At the frequency defined after the implementation of the first customer		C		
			Endpoint Detection and Response (EDR) Services - Operational Reports	Metrics of all scans conducted to include, at a minimum: number of unique devices scanned; scan dates; name of instance or device; total number of events; number of file deletions; and, number and disposition of quarantined records across all devices.	Daily	DIR, Customer	MSI Portal	Word	New	At the frequency defined after the implementation of the first customer		C		
			Endpoint Detection and Response (EDR) Services - Configuration Reports	Metrics on Malware infections and remediation Number of exclusions (i.e., files, file types, folders, partitions, etc. that are excluded from the scan), number of new exclusions, number of exclusions removed and business justification for all exclusions. Report showing definition files and currency levels of the devices, e.g., definition files at N/N+1 levels	Weekly	DIR, Customer	MSI Portal	Excel	New	At the frequency defined after the implementation of the first customer		C		
		STC-OPS-SMDM04	IDS/IPS - Operational Reports	Report of most frequent sources of blocked/detected inbound traffic sorted by volume High to Low Report of most frequent sourced geolocations of blocked/detected inbound traffic sorted by volume High to Low Report of most frequent destinations of blocked/detected inbound traffic sorted by volume High to Low Report of most frequent destination geolocations of blocked/detected inbound traffic sorted by volume High to Low Report of most frequent sources of blocked/detected outbound traffic sorted by volume High to Low Report of most frequent destinations of blocked/detected outbound traffic sorted by volume High to Low Report of most frequently activated filters - most blocks; sorted by volume - High to Low Report of most frequently activated filters - Permits and Blocks; sorted by volume - High to Low	Weekly	DIR, Customer	MSI Portal	Word	New	At the frequency defined after the implementation of the first customer		C		
		STC-OPS-SMDM05	IDS/IPS - Configuration Reports	Report of current IPS/IDS configuration settings, version information (SW and Filter), and summary of changes in the reporting period.	Monthly	DIR, Customer	MSI Portal	Word	New	At the frequency defined after the implementation of the first customer		C		
		STC-OPS-SMDM06	SMDM - Environment Review	Documented assessment of Customer's network architecture, protected systems, and applications and traffic patterns for each deployed Service including any findings as they relate to policy and signature settings. The report shall include recommendations and next steps for adjusting policy and signature components. Existing policy components and signatures for each custom policy deployed to the HIPS groups. Include any recommendations for signature and policy component updates. At a minimum, the report shall contain: a. Resulting analysis and reporting from the 6-month policy and architecture review. b. A summary discussion of new threats, trends, and proactive discoveries. c. An accounting of active signature-based settings on Service Provider's attack classification,	Semi-Annual	DIR, Customer	MSI Portal	Word	New	At the frequency defined after the implementation of the first customer		C		
		STC-OPS-SMDM07	HIPS - Operational Reports	Report of most frequent sources of blocked inbound traffic sorted by volume High to Low, Report of most frequent sources of blocked outbound traffic sorted by volume High to Low Report of most frequently activated filters - most blocks; sorted by volume - High to Low Report of most frequently activated filters - Permits and Blocks; sorted by volume - High to Low	Monthly	DIR, Customer	MSI Portal	Word	New	At the frequency defined after the implementation of the first customer.		C		
		STC-OPS-SMDM08	HIPS - Configuration Reports	Report of current HIPS configuration settings, version information (SW and Filter), and summary of changes in the reporting period.	Monthly	DIR, Customer	MSI Portal	Word	New	At the frequency defined after the implementation of the first customer		C		
		STC-OPS-SMDM09	Managed Firewalls - Configuration Reports	Report detailing the device configuration (SW version, filter sets if applicable) and summary of changes over the reporting period.	Monthly	DIR, Customer	MSI Portal	TBD	New	At the frequency defined after the implementation of the first customer		C		

											Report Data and Creation MSI publishes all reports. Column indicates who: (C) creates report for publication, (D) provides data to MSI			
Contract Reference	Report Category	Report ID	Report Name	Description	Frequency	Recipient	Report Location	Report Generator Tool	Existing or New Report	Report Start Date	MSI	Security Monitoring and Device Management	Incident Response	Risk and Compliance
		STC-OPS-SMDM10	WAF - Operational Reports	Report of most frequent sources of blocked inbound traffic sorted by volume High to Low, Report of most frequent sources of blocked outbound traffic sorted by volume High to Low Report of most frequently activated filters - most blocks; sorted by volume - High to Low Report of most frequently activated filters - Permits and Blocks; sorted by volume - High to Low	Monthly	DIR, Customer	MSI Portal	TBD	New	At the frequency defined after the implementation of the first customer		C		
		STC-OPS-SMDM11	WAF - Configuration Reports	Report of current HIPS configuration settings, version information (SW and Filter), and summary of changes in the reporting period.	Monthly	DIR, Customer	MSI Portal	Word	New	At the frequency defined after the implementation of the first customer		C		
		STC-OPS-SMDM12	SIEM - Operational Reports	Report summarizing and providing data for the SIEM including SIEM event counts per month, week, day or other time period required by the Customer with the counts broken down into the Customer's source categories. Number and types of alerts sent to Customer, Current list of all devices providing Syslog (feeds) to the SIEM for monitoring Number of events by device Summary of real time rule alerts in the past 30 days, including details for top 10 rules for which the most alerts were generated.	Monthly	DIR, Customer	MSI Portal	TBD	New	At the frequency defined after the implementation of the first customer		C		
		STC-OPS-SMDM13	MDS/MPS - Operational Reports	Report of most frequent sources of blocked/detected inbound traffic sorted by volume High to Low Report of most frequent destinations of blocked/detected inbound traffic sorted by volume High to Low Report of most frequent sources of blocked/detected outbound traffic sorted by volume High to Low Report of most frequent destinations of blocked/detected outbound traffic sorted by volume High to Low Report of most frequently activated filters - most blocks; sorted by volume - High to Low Report of most frequently activated filters - Permits and Blocks; sorted by volume - High to Low	Monthly	DIR	MSI Portal	Word, Excel	New	At the frequency defined after the implementation of the first customer		C		
		STC-OPS-SMDM14	MDS/MPS - Configuration Reports	Report of current MDS/MPS configuration settings, version information (SW and Filter) and summary of changes in the reporting period.	Monthly	DIR	MSI Portal	Word, Excel	New	At the frequency defined after the implementation of the first customer		C		
		STC-OPS-SMDM15	SOC Services - Operational Reports	Additional reporting exclusive of other SMDM reports documented in this Attachment 13-A as agreed upon and solutioned in the approved Customer Request for Solution	Monthly	DIR, Customer	MSI Portal	Word, Excel	New	At the frequency defined after the implementation of the first customer	C	D		
		STC-OPS-SMDM16	Log Management Device Report	Monthly report detailing the number of devices being logged.	Monthly	DIR, Customer	MSI Portal	Excel	New	Commencement Date		C		
		STC-OPS-SMDM17	Log Management Event Report	Monthly report detailing the number of events logged by device and amount of bandwidth used for logging	Monthly	DIR, Customer	MSI Portal	Excel	New	Commencement Date		C		
		STC-OPS-SMDM18	Targeted Threat Research Report	Report the threat analysis to the Customer in a format to be agreed upon by the Customer and Service Provider.	As Requested	DIR, Customer	MSI Portal	Word	New	At the frequency defined after the implementation of the first customer		C		
		STC-OPS-IRSP04	Advanced Threat Hunting One-Time Scan	Summary report of service activities, to include devices scanned, issues during the service and a summary of all findings with recommendations for remediation or security posture improvements.	One	Customer	At&T Sharepoint Portal	Word	New	At the end of service period			C	
		STC-OPS-SMDM19	Advanced Threat Hunting Subscription	Reports summarizing and providing data for the ATH Subscription including- ATH alert/notification counts per month, week, day, or other time period required by the Customer with the counts broken down into Customer's source categories. - Number and types of alerts sent to Customer, current list of all devices providing Syslog (feeds) to the SIEM for monitoring. -Number of events by device summary of real time rule alerts in the past 30 days, including details for top 10 rules for which the most alerts were generated.	Monthly	Customer	AT&T Sharepoint Portal	Word	New	At the frequency defined after the implementation of the first customer		C		
	Incident Response													
		STC-OPS-IRSP01	Security Incident Reporting	Details of all Security incident responses and activities, to include a timeline of events and activities.	As Requested	DIR, Customer	MSI Portal	Word, Excel	New	At the frequency defined after the implementation of the first customer			C	
		STC-OPS-IRSP02	Digital Forensics Report	Report on the results of digital forensics investigations in a format frequency to be mutually agreed upon by the IR Service Provider and Customer.	As Requested	DIR, Customer	MSI Portal	Word, Excel	New	At the frequency defined after the implementation of the first customer			C	
		STC-OPS-IRSP03	Response Preparedness Report	Provide Customer with a formal written report of the test results within thirty (30) days of each test. The content of the reports will be mutually determined by DIR and the Customer and the IR Service provider. At a minimum, each report shall include: a. The objective of the test; b. The results achieved; c. A comparison of the results to the measures and goals identified in the Security Response Plan; d. A plan and a schedule to remediate any Incident Response issues identified during testing.	As Requested	DIR, Customer	MSI Portal	Word	New	At the frequency defined after the implementation of the first customer			C	

											Report Data and Creation MSI publishes all reports. Column indicates who: (C) creates report for publication, (D) provides data to MSI			
Contract Reference	Report Category	Report ID	Report Name	Description	Frequency	Recipient	Report Location	Report Generator Tool	Existing or New Report	Report Start Date	MSI	Security Monitoring and Device Management	Incident Response	Risk and Compliance
	Risk & Compliance													
		STC-OPS-RCMP01	Penetration Testing Reports	Report detailing penetration testing results to include, at a minimum: systems tested; testing methodologies; results including specific sections on discovered vulnerabilities and critical or high risk vulnerabilities; potential impact of vulnerabilities; likelihood of the vulnerability being exploited; and suggested remediation of the vulnerability.	As Requested	DIR, Customer	MSI Portal	Word	New	Commencement Date				C
		STC-OPS-RCMP02	Risk Assessment Report	Risk assessment report, including but not limited to priorities, recommendations and a narrative of findings.	As Requested	DIR, Customer	MSI Portal	Word	New	Commencement Date				C
		STC-OPS-RCMP03	Cloud Compliance Scan Results	Documented results of compliance scans performed on cloud service providers	As Requested	DIR, Customer	MSI Portal	Word, Excel	New	At the frequency defined after the implementation of the first customer				C
		STC-OPS-RCMP04	Cloud Compliance Security Checklist Report	Documented results on the cloud provider's compliance to the security checklist.	As Requested	DIR, Customer	MSI Portal	Word, Excel	New	At the frequency defined after the implementation of the first customer				C
		STC-OPS-RCMP05	Cloud Compliance Security Checklist Response	Compliance answers from the security checklists.	As Requested	DIR, Customer	MSI Portal	Word, Excel	New	At the frequency defined after the implementation of the first customer				C
		STC-OPS-RCMP06	Vulnerability Scan Report	Report containing results from the vulnerability scan including recommended remediation activities to reduce security risks.	As Requested	DIR, Customer	MSI Portal	Word, Excel	New	Commencement Date				C
		STC-OPS-RCMP07	Web Application Vulnerability Scanning (WAVS) Report	Report containing results from the web application vulnerability scan, including web servers discovered and recommended remediation activities to reduce security risks.	As Requested	DIR, Customer	MSI Portal	Excel	New	At the frequency defined after the implementation of the first customer				C
		STC-OPS-RCMP08	Web or Mobile Application Penetration Testing Report	Report detailing web or mobile penetration testing results to include, at a minimum: systems tested; testing methodologies; results including specific sections on discovered vulnerabilities and critical or high risk vulnerabilities; potential impact of vulnerabilities; likelihood of the vulnerability being exploited; and suggested remediation of the vulnerability.	As Requested	DIR, Customer	MSI Portal	Word, Excel	New	At the frequency defined after the implementation of the first customer				C